

EXHIBIT 1

(Same as Def. Exhibit A-
Attachment #4 to Def. Motion
for Omnibus Relief,
Dkt. No. 32)

Search and Seizure Warrant

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

ORIGINAL

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

Case No. 5:15-MJ-273 (ATB)

Dacobe Enterprises LLC located at 325 Lafayette Street,)
 Utica, NY)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of New York (identify the person or describe the property to be searched and give its location):

Dacobe Enterprises LLC located at 325 Lafayette Street, Utica, NY described further in Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before August 3, 2015 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Andrew T. Baxter (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:

July 21, 2015 1:50 p.m. Andrew T. Baxter
 Judge's signature

City and state:

Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge

Printed name and title

Addendum attached.
 ATB

000001

Addendum to Search Warrant

Addendum to Search Warrant

1. **Minimization.** In executing the search of any computer or computer-related items authorized by this warrant, the law enforcement officers executing the search [hereinafter referred to as the "United States"] shall make reasonable efforts to utilize computer search methodology that avoids searching files, documents, or other electronically stored information which is not identified in the warrant.

2. **Completion of Computer Search.** The United States shall make an exact copy of all data and other electronically stored information from any seized data storage devices within thirty (30) days after the warrant is executed unless, upon a showing of good cause, such date is extended by order of this Court or any other court of competent jurisdiction.

3. **Return of Data.** If a resident or occupant of the premises from which a computer is seized pursuant to this warrant makes a written request to the United States for a return of the seized data storage devices, the United States shall provide such person within thirty (30) days of the receipt of such request with a copy of any requested data and electronically stored information that does not constitute contraband or instrumentalities of a crime or which has not been searched in accordance with paragraph 1 above. If the United States withholds any data or electronically stored information requested by any resident of the premises searched, the United States shall identify such withheld information or data to such resident and state the reason such data or information is not being returned.

4. **Return of Computer.** The United States shall determine within thirty (30) days of the execution of the warrant whether any seized computer contains any of the items for which the search was authorized or any contraband, instrumentalities of a crime, or property subject to forfeiture. If none is found, any such computer shall be returned forthwith to the premises from which it was seized.

5. **Retention of Rights.** Nothing in this warrant or this Addendum shall limit or prevent the United States from seizing any computer as contraband or as an instrumentality of a crime or from commencing forfeiture proceedings against a computer or the data contained therein. Moreover, nothing in this warrant or this Addendum shall limit or prevent any person from filing a motion for the return of seized property pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure or seeking any other relief such person deems appropriate.

Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))Dacobe Enterprises LLC located at 325 Lafayette
Street, Utica, NY)

Case No. 5:15-MJ-273 (ATB)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and seal under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of New York (identify the person or describe the property to be searched and give its location): Dacobe Enterprises LLC located at 325 Lafayette Street, Utica, NY described in Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252A, and the application is based on these facts: See Attached Affidavit

☒ Continued on the attached sheet.

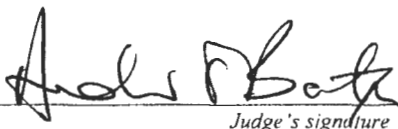
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Heather Weber, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: July 21, 2015


Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter U.S. Magistrate Judge
Printed name and title

U.S. DISTRICT COURT FOR THE NORTHERN DISTRICT OF NEW YORK
 I, the undersigned Clerk of the Court, do hereby certify that this is a true, correct and full copy of the original document on my custody.
 # of pages (incl. exhibits) 24
 Dated 7-31-2015
 by Lawrence K. Baerns, Deputy Clerk

000003

Affidavit in Support of an Application for a Search Warrant

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Heather Weber, a Special Agent with Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Federal Bureau of Investigation (FBI) Special Agent and have been employed in that capacity since February 2015. I am currently assigned to the Albany Division, Syracuse Resident Agency in Syracuse, New York. I have been involved in investigations and received training on a variety of criminal violations including the sexual exploitation of children and specifically violations of Title 18, United States Code, Section 2252A.
2. As a federal agent, I am authorized to investigate violations of United States laws and to execute search warrants issued under the authority of the United States.
3. This affidavit is made in support of an application for a warrant to search:
 - a. Dacobe Enterprises LLC of 325 Lafayette Street Utica, New York, herein referred to as SUBJECT PREMISES;
 - b. Computers and other electronic media located at the SUBJECT PREMISES during the execution of the search warrant.

for items, more particularly described in Attachment B, evidencing violations of:

- a. Title 18, United States Code, Section 2252A(a)(2)(A), which makes it unlawful to knowingly distribute or receive child pornography using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means including by computer; and

- b. Title 18, United States Code, Section 2252A(a)(5)(B), which makes it unlawful to knowingly possess or access with intent to view, any material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
4. The information contained in this affidavit is based upon information gathered by me as a part of the investigation as well as information provided to me by other Special Agents of the FBI involved in this investigation. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) are located at SUBJECT PREMISES, and within electronic media located therein.
5. At all times throughout this affidavit I use the term “child pornography” to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms “visual depiction”, “minor”, and “sexually explicit conduct” as those terms are defined in 18 U.S.C. § 2256 (see DEFINITIONS section below).

Peer to Peer

6. Peer to peer (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between

users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files currently being shared on the network. Ares, one type of P2P software, sets up its searches by keywords. The results of a keyword search using the Ares software are displayed to the user in the Ares program. The user then selects file(s) from the results for download to the user's computer. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the file. Typically, the file, once downloaded by the user, is made available for dissemination to other users of the Ares P2P software.

7. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he/she wants to download. The file is downloaded directly from the computer sharing the file. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain in that location until moved or deleted by the user.
8. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at

a time. For example, on one P2P network, Ares, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often however, a user downloading a file receives the entire file from one computer.

9. The Ares P2P network bases all of its file shares on the Secure Hash Algorithm (SHA1). SHA1 is a mathematical algorithm that allows for the fingerprinting of files. Once a file is checked with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that value will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.
10. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.
11. The computer running the file sharing application, in this case Ares, has an IP address assigned to it while it is on the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to determine the Internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the ISP. The following are facts known regarding the Ares file sharing network:

12. The Ares network is an open source public file-sharing network. Most computers that are part of the Ares network are referred to as nodes. A node can simultaneously provide files to some peers while downloading files from other nodes. Nodes may be elevated to temporary indexing servers referred to as “supernodes.” Supernodes increase the efficiency of the Ares network by maintaining an index of the contents of network peers. Ares users query supernodes for files and are directed to one or more peers sharing that file. There are many supernodes on the network; accordingly, if one shuts down the network continues to operate.
13. The Ares network can be accessed by computers running many different client programs, some of which include the original Ares Galaxy program, and derivatives compiled from the source code, which is open source and freely available. These programs (a/k/a “clients”) share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client. In this case, the user was using a version of Limewire to access the network.
14. During the installation of an Ares client, various settings are established which configure the host computer to share files. Depending upon the Ares client used, a user may have the ability to reconfigure some of those settings during installation or after the installation is completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other Ares users to download. This location is commonly referred to as the “My Shared Folder” or, colloquially, the “shared folder.” In many versions of Ares clients, the shared folder defaults to appear on the computer’s desktop.

15. The client software processes files located in a user's shared directory. As part of this processing, a SHA1 hash value is computed for each file in the user's shared directory. The client software processes files located in a peer's shared directory. As part of this processing, a SHA-1 hash value is loaded from a prior record or computed for each file in the user's shared directory.
16. The Ares network uses SHA-1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA-1 values to ensure exact copies of the same file are used during this process.
17. Upon connecting to the Ares network, a list of shared files, descriptive information and the files associated SHA-1 values are sent to the supernodes. This allows other users to locate these files. The frequency of updating information is dependent upon the client software being used and the Ares networking protocols. This information sent to the supernodes is only data about the file and not the actual file. The file remains on the user's computer. In this capacity, the supernode acts as a pointer to the files located on a user's computer.
18. When a download of a file is initiated, the user is presented with a list of users (nodes) who had told the Ares network that they have the requested file available for others to download. Typically, the supernodes and hosts computers on the network return this list containing node information and the IP addresses of computers which have reported they have the same file (based on SHA-1 comparison) or in some instances portions of

the same file available to others to download. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography.

19. Obtaining files from the Ares network, as described herein, returns the candidate list, including IP addresses, which can be used to identify the location of computers. Although the IP address is not usually visible to the end user in the common Ares clients, it is returned and used by the software to initiate the download. Law Enforcement has modified the Ares program to allow the downloading of a file from a single IP address as well as displaying the IP address which is known to all Ares clients, but not typically displayed within the Ares clients.

OVERVIEW OF THE INVESTIGATION

20. On March 23, 2015, your affiant was given information from the FBI Buffalo Field Office that an undercover Task Force Officer (TFO) had, on two separate dates, successfully downloaded files shared from the Ares network from a computer at IP address 64.65.206.37. Your affiant reviewed these files, and they are available for the Court's review upon request.

A. On September 24, 2014 between 3:03 pm and 3:14 pm, the undercover TFO downloaded two video files from IP 64.65.206.37, which are described as follows:

1. A file titled (pthc) sally-my daughter at 5 (fucking little girl)(hardcore)(2).mpg, is a video file depicting a prepubescent female child being vaginally penetrated by an adult male, who is lying behind her.

2. A file titled (yamad)hussyfan(pt)';'lhannah-forced h319(2)(2).mpg, is a video file depicting a prepubescent female child positioned in a chair by an adult male to get a close- up video image of her vagina and anus.

B. On October 15, 2014 between 12:29 pm and 12:36 pm, the undercover TFO successfully downloaded a file being shared by a computer at IP address 64.65.206.37. This is an image file depicting a naked prepubescent female lying on her back, with a naked prepubescent boy between her legs. What appears to be an Asian adult male is depicted standing near the boy, pointing at the girl's vagina.

C. On July 20, 2015 the undercover TFO was able to access the Ares network and review the videos and images available for download and sharing in the shared folder for IP address 64.65.206.37. This program allows the TFO to see the hash value, IP address and city location of users on the Ares network. The TFO was able to see that the user of this IP address has been an active user on Ares since 2011 and has been on the Ares network consistently over the past two weeks including on July 20, 2015. The TFO was also able to identify by hash value 156 files with known child pornography images and videos available for sharing by a computer at IP address 64.65.206.37 on July 20, 2015. Those files include:

- 1) An image depicting a pubescent female straddling an unknown male with his penis penetrating her vagina. This file is known child pornography that is part of the "Photo by Carl" series;
- 2) A video that is 2 minutes and 2 seconds in length that shows a nude prepubescent female lying on her back with her knees pulled up exposing her anus and vagina. The female exposes her vagina to the camera and an adult male

masturbates over her vagina until he ejaculates on the female's vagina and lower abdomen; and

3) A video file named (pthc)(orgasm) 6yr 8yr and 11 yr-encoded by sw!tch(2).avi that is 17 minutes and 35 seconds long. The video depicts a nude prepubescent female masturbating.

The TFO was unable to download any of the videos and images on July 20, 2015 because the program is limited by the number of open connections to the user available at the time it is reviewing those files. In essence the program got a busy signal when trying to download on July 20, 2015 as the ports available for sharing were all being used at the time.

21. On March 17, 2015, and July 20, 2015, FBI SA Kimberly Williams served a subpoena on EarthLink, for records for the registered owner of the IP address 64.65.206.37. On March 20, 2015, and July 21, 2015, EarthLink provided the following subscriber information:

Dacobe Enterprises LLC
325 Lafayette St
Utica, NY 13502
Point of Contact: Geoff Thorp, phone number 315-XXX-XXXX[redacted]

The information provided in the subpoena return also indicates that this IP address has been registered to the SUBJECT PREMISES since October 15, 2010.

22. The SUBJECT PREMISES is a two story, gray concrete building. There is no visible outside separate entrance to the second floor of the building. Checks with the utility company, National Grid, shows only one gas and electric account for the SUBJECT PREMISES, registered to Dacobe Enterprises, LLC. The United States Postal Service has confirmed that the address receives mail for only one business, Dacobe Enterprises

LLC, and two individuals Daniel Coby Beal, and his partner "Geoff." A Postal Service employee familiar with the location, indicates that Daniel and Geoff own the entire building, which houses a woodworking and acrylic business with 4 – 5 employees, and that they fabricate boxes and do acrylic melting in the upstairs portion of the building.

22. Dacobe Enterprises LLC has operated their business from the SUBJECT PREMISES since November 19, 2009.
23. On April 14, 2015, FBI Special Agent B. Mason Hughes visited publicly accessible areas of Dacobe Enterprises LLC. Dacobe Enterprises LLC is a manufacturing company that specializes in custom made display cases. He observed four computers and one office. There are two owners who stated they have 13 employees, and a workshop behind the building. Agent Hughes stood in the front of the company, which he described as the display, customer service area of the company. Agent Hughes did not see a separate entrance to the second floor of the building.
24. On June 26, 2015 your affiant went to the vicinity of the SUBJECT PREMISES to search for any open wireless networks in the proximity of the building. Using a Samsung Galaxy S5, three wireless networks were identified from the sidewalk, in front of the SUBJECT PREMISES. All but one of the wireless networks found were secured; the open network connection related to an adjacent business, Metzler Printing.

DEFINITIONS

25. The following definitions apply to this Affidavit:
 - a. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

- b. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e) (1).
- c. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- d. “node” is a connection point, a redistribution point or a communication endpoint (some terminal equipment).
- e. “App” is an electronic application created by a company that allows users to access the service through a mobile device.
- f. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- g. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).
- h. “log file” refers to the file to which a computer system writes a record of its activities.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. Based on my review of the files of similar FBI investigations and conversations that I have had with other federal agents, including FBI SA Alix Skelton, who has been investigating child exploitation crimes for three years, and who has been involved in numerous search warrants, subject interviews, arrests and prosecutions of individuals engaged in child exploitation and child pornography offenses, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography usually do so by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography.
27. Collectors of child pornography typically retain their materials and related information for many years. Most collectors of child pornography seek to increase the size of their collections in a manner similar to collectors of coins, stamps, or rare books. Many retain these materials, including information regarding sources, for their entire adult lives. Moreover, individuals who distribute and/or collect child pornography generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Additionally, collectors of child pornography rarely destroy correspondence from other collectors or distributors unless their activities are detected by law enforcement or other authorities.
28. Collectors of child pornography often correspond and/or meet with others to share information and materials, rarely destroy correspondence from other child pornography distributors or collectors, conceal such correspondence and sexually explicit material,

and often maintain lists of names, addresses, telephone numbers, and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

29. Accordingly, information used to support probable cause is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time. Thus, information used to support probable cause in child pornography cases is often not deemed stale, even if somewhat old, because collectors and traders of child pornography are known to store and retain their collections and correspondence related to their collections for extended periods of time.
30. Based on information provided to me by other law enforcement officers, I know that persons who collect and distribute child pornography:

- a. Frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides, and/or drawings or other visual media that they use for their own sexual arousal and gratifications.
- b. May receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or in other visual media) or from literature describing such activity.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

31. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most

or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, thumb drives, SD and media cards, and others) can store the equivalent of thousands of pages of information. In particular, when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
33. Furthermore, because there is probable cause to believe that the computers, personal devices and their storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2252 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED


34. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - a. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents;
 - e. scanning storage areas;
 - f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear that violate the cited laws; and
 - g. performing any other data analysis technique that may be necessary to locate and retrieve evidence the aforementioned laws were violated.
35. Dacobe Enterprises LLC is a functioning company. The seizure of Dacobe Enterprises LLC's computers may limit its ability to conduct legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media must be seized and what computers and storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

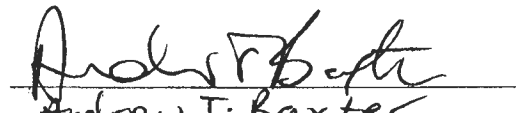
CONCLUSION

36. Based upon the above information, your affiant respectfully submits that there is probable cause to believe that someone using the Internet account subscribed to by

Dacobe Enterprises LLC at the SUBJECT PREMISES, is involved in the distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. § 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. § 2252A is located in the SUBJECT PREMISES, and that evidence of those violations exist and are concealed on the SUBJECT PREMISES and within computers, computer equipment and/or electronic media located therein. Accordingly, your affiant respectfully requests that the attached warrant be issued authorizing the search of the SUBJECT PREMISES and any computers, computer equipment, or computer storage media and electronic storage media located during the search, for the items listed in Attachment B.


Special Agent Heather Weber
Federal Bureau of Investigation

Sworn and subscribed before me
this 21st day of July, 2015.


Andrew T. Baxter
United States Magistrate Judge

ATTACHMENT A

Places to be Searched

The place and items to be searched:

1. Dacobe Enterprises LLC, located at 325 Lafayette Street in Utica, New York. Adjacent to the business on the west side is a company, Fisher Auto Parts. The SUBJECT PREMISES is a concrete front, mostly off-white, two-story building with an indented business entrance facing the street on the north side. The east side of the building is red brick with another, more frequently used entrance and includes with a brown, aluminum structure connected to the rear of the store. The search includes storage areas located at the SUBJECT PREMISES.



ATTACHMENT B

Items to be Seized

Items evidencing violations of Title 18, United States Code, Sections 2252A (distributing, receiving, viewing or possessing child pornography).

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer and electronic hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer and electronic hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives, secure digital (sd) cards, and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); digital cameras; related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices,

mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.
8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic

records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone) and ISPs. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, USB drives, secure digital (“SD”) cards, or other memory storage devices.

Documents, Computer, and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, notes, and reference materials.
10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.
11. Records of address or identifying information for the target(s) of the investigation, and any Ares names (a.k.a., “Nics”), user IDs, eIDs (electronic ID numbers), and passwords.
12. Documents and records, including, for example, receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the residence and/or possession of the searched items located therein.

13. Computer records and evidence identifying who the particular user was who distributed, transmitted, downloaded or possessed any child pornography found on any computer or computer media.

• **Materials Relating to Child Pornography, Child Erotica, and Depictions of Minors**

14. Any and all child pornography, and any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors, as those terms are defined in Title 18, United States Code, Section 2256.

15. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

16. Any records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

17. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes.

Photographs of Search

18. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

Government's Sealing Application

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

In Re . . .

Search Warrant

) Criminal No. 5:15-MJ-273 (ATB)
)
) **Government's Sealing Application**
)
) **Filed Under Seal**
)
)
)

The United States of America, by and through its counsel of record, the United States Attorney for the Northern District of New York ["NDNY"], hereby applies to the Court pursuant to NDNY Criminal Local Rule 13.1 for the sealing of the following: (a) one or more documents submitted to the Court at the same time as this sealing application, which document(s) request a Court order authorizing certain investigative activity or an arrest warrant; (b) the Court's order authorizing such investigative activity or an arrest warrant; (c) this sealing application; and (d) the Court's sealing order, which has the same caption.

The United States respectfully requests such sealing because public filing of the above-described documents may *[indicate all reasons that apply]*:

<input checked="" type="checkbox"/>	Jeopardize an ongoing federal criminal investigation by revealing the existence of that investigation to potential targets and subjects of the investigation;
<input type="checkbox"/>	Jeopardize the safety of a person who has provided information and/or other assistance to the criminal investigation or the family and/or friends of such person by revealing such person's cooperation with the investigation to those under investigation or their associates;
<input checked="" type="checkbox"/>	Jeopardize the safety of law enforcement personnel;
<input type="checkbox"/>	Reveal law enforcement methods, techniques, and/or procedures, thereby jeopardizing future investigations using such methods, techniques, and/or procedures;
<input type="checkbox"/>	Reveal non-public information about one or more victims and/or witnesses and such information could lead to adverse financial and/or social consequences for such person(s);
<input type="checkbox"/>	Reveal non-public information about one or more targets or subjects of the investigation who have not been charged with a crime in the relevant investigation and such information could lead to adverse financial and/or social consequences for such person(s);
<input type="checkbox"/>	Reveal matters in violation of federal law, such as Rule 6(e) of the Federal Rules of Criminal Procedure and/or Title 26, United States Code, Section 6103;
<input type="checkbox"/>	Jeopardize national security.

Search Warrant Return

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 5:15-MJ-273 (ATB)	Date and time warrant executed: 7/29/15 @ 11:00 AM	Copy of warrant and inventory left with: Geoff Thorp
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: auto;"><div>U.S. DISTRICT COURT - N.D. OF N.Y.</div><div style="text-align: center; font-size: 1.2em; font-weight: bold;">FILED</div><div style="text-align: center; border: 1px solid black; padding: 2px; margin: 2px 0;">AUG - 5 2015</div><div>AT _____ O'CLOCK</div><div>Lawrence K. Baerman, Clerk - Syracuse</div></div>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: <u>8/5/15</u></p> <div style="text-align: right;"><div><u><i>Heather Weber</i></u> Executing officer's signature</div><div><u>Heather Weber Special Agent</u> Printed name and title</div></div>		

000028

Receipt for Seized Property (Dacobe Enterprises LLC)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/SeizedFile # 305I-AL-6324781On (date) July 29, 2015

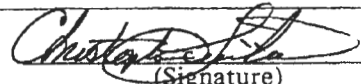
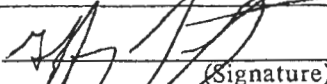
item(s) listed below were:

- ☐ Received From
☐ Returned To
☐ Released To
☒ Seized

(Name) DACORE ENTERPRISES LLC.(Street Address) 325 LA FAYETTE STREET.(City) UTICA, NEW YORK

Description of Item(s):

- I. 3 (THREE) MEMOREX DVD+R's.
- II. 1 (ONE) TOSHIBA LAPTOP COMPUTER SN# 99282687 K
- III. 1 (ONE) SAMSUNG CELLULAR TELEPHONE
- IV. 3 (THREE) THUMBDRIVES: PNY 8GB, PNY ATACHE, DATARANGER 512MB
- V. 1 (ONE) HPM 8000 CPU; SN: CNX737MVM
- VI. 1 (ONE) TOSHIBA EXTERNAL HD SN: Z4QYS8103TT1
- VII. 1 (ONE) ANTEC COMPUTER (CPU)
- VIII. 1 (ONE) GREY, SONY CYBER-SHOT CAMERA 369400, BLACK, SONY BATTERY CHARGE
x374686
- IX. 1 (ONE) SONY 32MB Memory Stick.

07.29.2015Received By: 
(Signature)Received From: 
(Signature)